UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,510	10/31/2001	Richard Paul Tarquini	10017331-1	7297

7590 05/19/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ZIA, SYÉD	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

6

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/003,510
Filing Date: October 31, 2001
Appellant (s): TARQUINI ET AL.

James L. Baudino
Registration No. 43,486
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 22, 2006 appealing from the Office action mailed July 14, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

This appeal involves claims 1-16.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

A copy of the appealed claims 1-16 appears on pages in the Appendix to the appellant's brief is correct.

(8) Evidence Relied Upon

6,704,874	Porras	03-2004
6,453,345	Trcka et al.	09-2002

(9) Grounds of Rejection

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claim 10 is rejected under 35 U.S.C. 102(e) as being anticipated by Porras (U. S. Patent 6,704,874).

2. Regarding Claim 10 Porras teaches a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method [Fig.6, col.9 line 1 to line 20]:

identifying [sensors 22 monitoring various host/network traffic for suspicious activities] frame [streams] as an intrusion by an intrusion detection application (col.3 line 30 to line 37, and col.3 line 54 to col.4 line 1);

decoding [translation module 32] by the intrusion delectation application, the intrusion-related data (col.4 line 1 to line 25).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-9, and 11-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras (U. S. Patent 6,704,874), and further in view of Trcka et al (U. S. Patent 6,453,345).

4. Regarding Claim 1 Porras teaches a method of detecting network-intrusions [detecting suspicious activities, such as intrusion, and based on that generating digital alerts] (Fig.1 Item 22, and col.1 line 26 to line 28) at a first node of a network [Fig.1, item 12], comprising:

identifying [sensors 22 monitoring various host/network traffic for suspicious activities] frame [streams] as an intrusion by an intrusion detection application (col.3 line 30 to line 37, and col.3 line 54 to col.4 line 1);

archiving event-data [raw, unprocessed alerts] associated with the frame [steams]; and

decoding [translation module 32] the event-data by a decode engine [aggregation, that is combining alerts produced by a single monitoring sensor] (col.6line 2 to line 5), the decode engine integrated within the intrusion detection application (col.4 line 1 to line 25).

Although the system disclosed by Porras shows all the features of the claimed limitation, but Porras does not specifically disclose *archiving* (for passive analysis) of network alerts, such as network intrusion, of network traffic.

In an analogous art, Trcka, on the other hand discloses a network security and surveillance system passively monitoring surveillance traffic, such as network intrusion, by routing surveillance traffic [raw, unprocessed alerts] to Archival Media Unit (process 64, and item 80, Fig.3), such as database, and using archival data processing method for analysis (Fig.3, col.11 line 27 to line 48).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Porras and Trcka, because Trcka's method of archiving network traffic data would not only promote audit trail of a successful security attack in the system of Porras during monitoring of network intrusion but will also provide extent of damage caused by intrusion traffic by performing playback (passive analysis) from traffic analysis of archived intrusion data, and thus not putting extra burden on latency of network traffic.

5. Claims 2, 5-6 are rejected applied as above in rejecting Claim 1. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 2, providing, by a network filter service provider (Porras: item 54, Fig.2) of the intrusion detection application, the event-data to an event-database (Porras: col.4 line 27 to line 40).

As to claim 5, generating a report from the decoded event-data; and providing the report to a report viewer (Porras: col.6 line 33 to line 52).

As to claim 6, providing, by the intrusion detection application, the decoded event-data to an intrusion detection client application (Porras: col.7 line 33 to line 55).

6. Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras (U. S. Patent 6,704,874), as applied to claim 10, and further in view of Trcka et al (U. S. Patent 6,453,345).

Regarding Claim 11-13 Porras teaches a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method [Fig.6, col.9 line 1 to line 20] of:

- generating a report from the decoded intrusion related data (col.6 line 33 to line 52).

Although the system disclosed by Porras shows all the features of the claimed limitations, but Porras does not specifically disclose *archiving decoded (identified) data* (for passive analysis) of network alerts, such as network intrusion, of network traffic.

In an analogous art, Trcka, on the other hand discloses a network security and surveillance system passively monitoring surveillance traffic, such as network intrusion, by routing surveillance traffic [raw, unprocessed alerts] to Archival Media Unit (process 64, and item 80, Fig.3), such as database, and using archival data processing method for analysis (Fig.3, col.11 line 27 to line 48).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Porras and Trcka, because Trcka's method of archiving network traffic data would not only promote audit trail of a successful security attack in the system of Porras during monitoring of network intrusion but will also provide extent of damage caused by intrusion traffic by performing playback (passive analysis) from traffic analysis of archived intrusion data, and thus not putting extra burden on latency of network traffic.

7. Claims 3, 7-9, and 14 are rejected applied as above in rejecting Claims 2, 6, and 11. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 3, providing the event-data to a decode server [remote processing center 26(server)] (Porras: col.4 line 33 to line 40).

As to claim 7, wherein the decoded event-data is formatted, by the client application, for display in a graphical user interface (Porras: col.7 line 19 to line 33).

As to claim 8, wherein the intrusion detection application runs locally on the first node [Fig.1 item 22 of network node 12] (col.3 line 19 to line 22).

As to claim 9, wherein the intrusion detection client application runs remotely on a second node, the first node and the second node operable to engage in a communication session between the client application and the intrusion detection application (Porras: col.3 line 30 to line 40, and col.7 line 19 to line 32).

As to claim 14, wherein the instruction set, when executed by the processor, further causes the processor to perform the computer method of transmitting the decoded data to a client application (Porras: col.7 line 33 to line 55).

8. Claims 4, and 15 are rejected applied as above in rejecting Claims 3, and 14. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 4, wherein the decode server obtains the event-data from at least one of an event viewer and a report server [remote management interface 36] (Porras: col.3 line 23 to line 30, and col.6 line 28 to line 33).

As to claim 15, wherein transmitting the decoded data to a client application further comprises transmitting the report to a client application in communication with the intrusion detection application (Porras: col.3 line 30 to line 40, and col.7 line 19 to line 32).

9. Claim 16 is rejected applied as above in rejecting Claims 15. Furthermore, the system of Porras, and Trcka teaches and describes a system analyzing network intrusion, further comprising:

As to claim 16, wherein transmitting the report to a client application further comprises transmitting the report to the client application in communication with the intrusion detection application (Porras: col.7 line 33 to line 55), the client application running remotely from the intrusion detection application (Fig.4, col.3 line 23 to line 26).

(10) Response to Argument

1: First Ground of Rejection (Claims 1-9)

It is argued by the Appellant that "the translation module 32 of Porras relied on by the Examiner is not integrated within the monitoring system 22 of Porras as is required by Applicants' Claim 1 (emphasis added). To the contrary, the Examiner relies on the monitoring system 22 of Porras as corresponding to the "intrusion detection application" recited by Claim 1 but offers no support or showing that the translation module 32 of Porras relied on by the Examiner as corresponding to the "decode engine" recited by Claim 1 is <u>integrated within</u> the monitoring system 22 of Porras ".

The examiner respectfully disagrees. Regarding this argument, examiner emphasis that the system of Porras teaches a network based alert management system 10 that includes plurality of networks (12, 14, and 16). Each of the networks 12-14 includes security and fault monitoring systems 22. Each security and fault monitoring system 22 is linked (i.e. interconnected, for example, by cable transport connection/communication lines 30) to an alert manager 24. The alert manager 24 includes a receive-input logic module 28. The receive-input logic 28 of the alert manager 24 is equipped with translation modules 32 to translate the original, raw alert streams from the monitors 22 into a common format for further processing. Therefore, in this network based alert management system the fault monitoring system 22 is completely and directly integrated with translation module 32 (emphasis added) (Fig.1 col.3line 15 to line 30, and col.4 line 11 to line 26). Furthermore, the formatted alerts are passed 54 through user-specified filters and alerts not matching criteria of the user-specified filters are discarded. The alert manager 24 and other components of the alert management network 10 may be implemented and executed on a wide variety of digital computing platforms, for example, workstation-class computer hardware and operating system software platforms such as Linux, Solaris, Unix, and Windows (emphasis added) (Fig.1 col.3 line 62 to col.4 line 17,and col.9 line 1 to line 6).

Appellant further argued, "Trcka et al. does not remedy the above-reference deficiencies of Porras".

Regarding this argument, examiner respectfully disagrees, and state that the Examiner did not rely on Trcka to teach the above mentioned claimed limitation. Trcka was specifically relied on to disclose *archiving* (for passive analysis) of network alerts, such as network intrusion, of network traffic.

For these reasons, it is believed that the system of Porras and Trcka teaches the applicant's language of claims 1-9.

2: Second Ground of Rejection (Claim 10)

Regarding Claim10 The Appellant has indicated that that as discussed above on connection with independent Claim 1, Porras appears to disclose that the monitoring system 22 of Porras includes an intrusion detection system for monitoring various host and/or network activity and generating a stream of alerts triggered by potentially suspicious events or malicious intrusions within the networks 12-16 of Porras (column 3, lines 30-32 and 54-61).

Appellant further argue, Claim 10 recites, "identifying, by an intrusion detection application, a frame of data as intrusion-related" and decoding, by the intrusion detection application-, the intrusion-related data" (emphasis added). The Examiner relies on the monitoring system 22 of Porras as corresponding to the intrusion detection application" recited by Claim 10 but offers no support or showing that such monitoring system 22 of Porras " decod[es]. . . the intrusion-related data" as is required by Applicants' Claim 10. To the contrary, the Examiner relies on the remote translation module 32 of Porras for supplying such decoding, yet the translation module 32 of Porras clearly is not part of the monitoring system 22 of Porras".

The examiner respectfully disagrees. Regarding this argument, examiner emphasis that the system of Porras teaches a network based alert management system 10 that includes plurality of networks (12, 14, and 16). Each of the networks 12-14 includes security and fault monitoring systems 22. Each security and fault monitoring system 22 is linked (i.e. interconnected, for example, by cable transport connection/communication lines 30) to an alert manager 24. The alert manager 24 includes a receive-input logic module 28. The receive-input logic 28 of the alert manager 24 is equipped with translation modules 32 to translate the original, raw alert streams from the monitors 22 into a common format for further processing. Therefore, in this network based alert management system the fault monitoring system 22 is completely and directly integrated with translation module 32 (emphasis added) (Fig.1 col.3line 15 to line 30, and col.4 line 11 to line 26). Furthermore, the method of managing alerts by the alert manager 32 in a network includes receiving alerts from network sensors, consolidating, and generating output reflecting the consolidated alerts (Fig.1 col.3 line 62 to col.4 line 17).

3: First Ground of Rejection (Claims 11-16):

It is argued by the Appellant that "Claims 11-16 depend from independent Claim 10, and as discussed above, Claim 10 is patentable over the Porras reference, and further state that, Porras does not disclose or even suggest identifying, by an intrusion detection application, a frame of data as intrusion-related and decoding, by the intrusion detection application, the intrusion-related data (emphasis added)".

The examiner respectfully disagrees. Regarding this argument, examiner emphasis that the system of Porras teaches a network based alert management system 10 that includes plurality of networks (12, 14, and 16). Each of the networks 12-14 includes security and fault monitoring systems 22. Each security and fault monitoring system 22 is linked (i.e. interconnected, for example, by cable transport connection/communication lines 30) to an alert manager 24. The alert manager 24 includes a receive-input logic module 28. The receive-input logic 28 of the alert manager 24 is equipped with translation modules 32 to translate the original, raw alert streams from the monitors 22 into a common format for further processing. Therefore, in this network based alert management system the fault monitoring system 22 is completely and directly integrated with translation module 32 (emphasis added) (Fig.1 col.3line 15 to line 30, and col.4 line 11 to line 26). Furthermore, the receive-input logic 28 of the alert manager 24 which is equipped with translation modules 32 (i.e. decoding) translate the original, raw alert streams from the monitors 22 into a common format for further processing. The formatted alerts are passed 54 through user-specified filters and alerts not matching criteria of the user-specified filters are discarded (emphasis added) (Fig.1 col.3 line 62 to col.4 line 17).

Appellant further argued, "Trcka et al. does not remedy the above-reference deficiencies of Porras".

Regarding this argument, examiner respectfully disagrees, and state that the Examiner did not rely on Trcka to teach the above mentioned claimed limitation. Trcka was specifically relied on to disclose *archiving* (for passive analysis) of network alerts, such as network intrusion, of network traffic.

For these reasons, it is believed that the system of Porras and Trcka teaches the applicant's language of claims 11-16.

(11) Related Proceedings Appendix

No decision rendered by a court of the Board is identified by the examiner in the Related Appeals and Interferences section of the examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Syed A. Zia (Examiner AU 2131)

Conferees:

Justin T. Darrow (Primary Examiner AU 2132)

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Gilberto Barron Jr. (SPE AU 2132)